Cloned in Seconds: Why Legacy Access Cards, Readers, and Wiring Are a Security Risk

---

A White Paper on the Evolving Threat Landscape in Access Control
October 2025

Prepared by Steve Gocinski
Principal Security Strategist & Systems Architect
Fire and Security Services Corporation

Executive Summary

Since 1974, 125 kHz proximity cards and the Wiegand wiring protocol have served as the de facto standard for physical access control systems. They were reliable, cost-effective, and became the backbone of secure facility entry for decades.

But technology never stands still—and neither do those who exploit it.

Today, low-cost RFID cloning devices, often available online for under $30, can duplicate unencrypted access cards in seconds.[1] Social media and open-source communities now openly share methods that once required specialized knowledge. As a result, what was once considered “secure enough” has quietly become a known vulnerability.

This paper explains, in plain language, how legacy card and reader technology can be compromised, how modern encrypted credentials and communication protocols solve those issues, and what a responsible, standards-aligned upgrade path looks like.

Real-World Exploits: Proof, Not Theory

These aren’t lab demonstrations—they’re public, documented incidents.

- **Hotel Key Cloned in 10 Seconds (WIRED):** A cybersecurity researcher demonstrated that a standard hotel keycard could be copied using a $30 handheld RFID device, granting unauthorized room access in seconds.[1]
- **University Fob Cloning (WRAL News):** A student at the University of North Carolina at Chapel Hill was charged with multiple felonies after allegedly using a low-cost RFID tool to clone campus key fobs, providing access to restricted areas.
- **Long Island Rail Road Time Fraud (MTA Inspector General, 2025):** An internal investigation found that employees used cloned ID cards—created with devices purchased online for under $30—to falsify time entries and gain unauthorized facility access. The report cited the widespread availability of cloning tools and the continued use of unencrypted proximity cards as key factors enabling the scheme.[15]
- **Retail Card Duplication (Home Depot / Lowe’s):** Major hardware retailers now offer in-store kiosks and services that will copy many common low-frequency (125 kHz) access cards and fobs from the original presented credential. These services make cloning trivial—no specialized tools or expertise required—but they cannot duplicate modern, encrypted 13.56 MHz smart cards (e.g., Seos / DESFire) that use mutual authentication and AES encryption.

Each example highlights how common, existing proximity technologies—which still account for the majority of supported credential technologies among surveyed companies—can be compromised with inexpensive, easily concealed devices.[2]

Why This Matters to Businesses

Most offices and facilities still rely on the same underlying technology first introduced nearly fifty years ago. These systems broadcast card data in clear text, and the wiring that connects the reader to the control panel sends that same information without encryption or supervision.[1]

With cloning tools now widely available and tutorials circulating online, the risk is no longer hypothetical—it's systemic.[4]

Organizations that continue to use demonstrably compromised systems may face questions from insurers or regulators about whether they've addressed known, preventable security weaknesses.[5]

The technology still functions, but it no longer aligns with modern security expectations for securing physical assets and data environments.[7]

How the Vulnerability Works (Simplified)

Legacy 125 kHz Cards

When a card is presented to the reader, it transmits a fixed identification number—unencrypted and unchanging.[1] Any device within range of a card can capture that ID, a process known as signal sniffing or eavesdropping, and reproduce it on another card in seconds using readily available RFID copiers.[1]

Wiegand Reader Wiring

The Wiegand protocol, invented in 1974, transmits data from the reader to the controller using simple, two-wire data lines.[3] This communication is sent entirely in plaintext.[3] Anyone who gains brief access to that wiring can attach a small eavesdropping device (such as the ESP Key, purchasable for under $100) to record credentials (including the facility code and user ID).[3] The attacker can then wirelessly replay the captured credential to gain unauthorized entry—a Replay Attack.[3] Furthermore, Wiegand is unidirectional and provides no supervision, meaning the control panel cannot detect if the reader has been tampered with, disabled, or disconnected.[3]

Together, either of these weaknesses allow unauthorized users to mimic legitimate badges without detection—and the system has no way to tell the difference.

Modern Standards That Close the Gap

Encrypted Seos-Class Credentials

Next-generation credentials such as Seos and MIFARE DESFire EV2/EV3 employ AES-128-bit encryption and mutual authentication.[9] AES-128 is the global standard for secure data encryption used in banking and government applications.[10]

The credentials store data using advanced encryption, making them virtually impossible to duplicate using off-the-shelf cloning devices.[9]

Seos, supported by 18% of organizations, also uses Standards Based Cryptography and can be software-upgraded to combat future security threats.[2]

The same credential platform supports both card and mobile formats, enabling future flexibility and secure identity management.[9]

OSDP Secure Channel Readers

The Open Supervised Device Protocol (OSDP)—approved as international standard IEC 60839-11-5—replaces Wiegand's one-way, unencrypted signaling.[3]

- **Encrypted Communication:** OSDP mandates the use of AES-128 encryption for all communication between the reader and the controller, transforming captured data into unusable ciphertext.[3] This eliminates data interception and replay attacks.[8]
- **Bidirectional Communication and Supervision:** OSDP enables two-way communication, allowing the controller to constantly monitor the reader's status. This supervision provides real-time alerts against tampering or disconnects, an essential feature Wiegand lacks.[3]
- **Firmware Updates:** OSDP readers can receive firmware updates to stay ahead of evolving threats and improve user experience.
- **Centralized Management:** Bidirectional communication allows for centralized pushing of software and firmware updates to all readers simultaneously, drastically reducing maintenance labor and costs.[3]

Together, Seos-class credentials and OSDP Secure Channel readers bring physical access control up to the same encryption and authentication standards long used in banking.

Technical Comparison: Wiegand vs. OSDP

Feature	Legacy Wiegand Protocol	OSDP Standard
Encryption	None (Plaintext Data)	AES-128 Encryption [4]
Communication	Unidirectional (One-way)	Bidirectional (Two-way) [4]
Tamper Detection	No (Cannot detect disabled readers)	Yes (Controller monitors status) [4]
Data Interception	Easy to intercept credentials	Encrypted to prevent interception [9]
Max Cable Length	Approx. 500 feet	Up to 4,000 feet [4]
Centralized Updates	No (Requires physical connection)	Yes (Software updates pushed centrally) [4]

Implementation Considerations

Modernization does not require starting from scratch. Leading manufacturers offer products designed for a smooth transition.[3]

Infrastructure Validation: While OSDP cabling should ideally be low-capacitance shielded wire, existing Wiegand-style cabling can often be reused. Industry guidance suggests the risk is significantly less if the cable run is less than 200 feet.[3] This criterion allows for strategic reuse of infrastructure, minimizing re-cabling costs.

Reader Upgrade: Replace legacy readers with multi-technology OSDP Secure Channel models capable of encrypted, supervised communication.[12]

Credential Issuance: New encrypted credentials (such as multi-technology cards) are issued to users.[10] During migration, upgraded readers can temporarily accept both legacy and new credentials to ensure a smooth transition.[11] Mobile credential capability is also supported for future flexibility.

Panel Compatibility: Some legacy controllers can be upgraded via door-board or firmware replacement to support OSDP.[3]

Phased Execution: Facilities typically modernize high-priority entry points first, such as data centers or executive areas, followed by secondary areas, to maintain continuity and manage capital expenditure.[3]

The Practical Benefits

- **Prevents Cloning and Replay Attacks:** Encrypted credentials and OSDP communication close known, trivial exploitation paths.[8]
- **Provides Tamper Visibility:** OSDP's continuous supervision ensures the system can immediately detect when a reader is removed or compromised, mitigating risk in real time.[3]
- **Supports Future Technology:** Encrypted readers and OSDP accommodate mobile credentials, cloud integrations, and biometrics without further rewiring.[3]
- **Maintains Operational Continuity:** Users experience the same swipe or tap action; administrators gain higher security assurance and simplified management due to centralized updates and long-distance cabling support.[3]

Summary

Legacy proximity systems were the right choice for their time, but the threat landscape has changed. The continued reliance on unencrypted 125 kHz cards and the Wiegand protocol creates a critical, unnecessary, and exploitable security risk.

Modern encryption standards now make cloning and interception effectively impractical—and they're becoming the new baseline expected by insurers, regulators, and enterprise security teams.

Upgrading to Seos-class encrypted credentials and OSDP Secure Channel readers delivers a measurable improvement in security posture while strategically preserving existing infrastructure where technically feasible.

Recommendations

In today's security landscape, Wiegand is no longer a viable option for new installations. Organizations should transition to OSDP readers for better security, reliability, and future scalability.

• Evaluate your current access control infrastructure. If you're currently using Wiegand, start planning a migration strategy. Determine whether a full OSDP migration or phased approach is the best option.

•For new installations, choose OSDP readers whenever possible to ensure encrypted, tamper-resistant communication.

Works cited

1. The Truth About Card Cloning - CDVI UK | Blog, accessed October 24, 2025, https://www.cdvi.co.uk/blog-the-truth-about-card-cloning/
2. The 2024 State of Physical Access Trend Report - ASHB - Association for Smarter Homes & Buildings, accessed October 24, 2025, https://www.ashb.com/wp-content/uploads/2024/10/IS-2024-175.pdf
3. There Is a Hole in the Boat: Why Access Control Professionals Need ..., accessed October 24, 2025, https://www.securityindustry.org/2021/11/09/there-is-a-hole-in-the-boat-why-access-control-professionals-need-to-move-from-wiegand-to-osdp/
4. The 125kHz Proximity Card Dilemma - ict.co, accessed October 24, 2025, https://ict.co/blog/the-125khz-proximity-card-dilemma/
5. Data Protection Law: An Overview - Congress.gov, accessed October 24, 2025, https://www.congress.gov/crs-product/R45631
6. Cyber Insurance and Security: Meeting the Rising Threat - KnowBe4, accessed October 24, 2025, https://www.knowbe4.com/hubfs/Insurance-Report-WhitePaper-2025-EN-US_F.pdf
7. Data Security Breaches: A Legal Guide to Prevention and Incident Response, accessed October 24, 2025, https://www.svlg.com/news-resources/data-security-breaches-a-legal-guide-to-prevention-and-incident/
8. Why choose OSDP over Wiegand in access control | White Paper ..., accessed October 24, 2025, https://whitepapers.axis.com/en-us/osdp-protocol-in-access-control
9. AN INTRODUCTION TO CARD TECHNOLOGY - ColorID, accessed October 24, 2025, https://www.colorid.com/uploads/4/2/2/9/42295857/technology_cards.pdf
10. Understanding HID Security Card Types - Telaeris, Inc., accessed October 24, 2025, https://telaeris.com/understanding-hid-security-card-types
11. HID® Seos®/MIFARE® DESFire® EV2 5906 - HID Global, accessed October 24, 2025, https://www.hidglobal.com/products/seos-mifare-desfire
12. The Benefits of OSDP | Sonitrol, accessed October 24, 2025, https://www.sonitrol.com/blog/benefits-osdp
13. EOL & Security Notices - Honeywell Building Technologies, accessed October 24, 2025, https://buildings.honeywell.com/au/en/brands/our-brands/security/support-and-resources/product-resources/eol-and-security-notices
14. Access Control Market Size & Share | Industry Report, 2030 - Grand View Research, accessed October 24, 2025, https://www.grandviewresearch.com/industry-analysis/access-control-market-report
15. They Can't Do Nothing To Us': LIRR Employees Manufactured, Sold, and Used Cloned Swipe Cards to Get Paid While Not Working October 23, 2025

https://mtaig.ny.gov/News/10.LIRRClonedCards.102325.pdf

About Fire and Security Services Corporation

Fire and Security Services Corporation (FSS) provides complete security and life safety solutions that protect people, property, and operations.

From access control, intrusion detection, CCTV, analytics, and integrated security management to fire alarm and other life safety systems, FSS delivers trusted protection for commercial, residential, industrial, and institutional facilities across the United States and Canada—as well as globally through its network of international partners.

As a full-service provider, FSS handles system design, installation, and maintenance with a commitment to technical excellence and client partnership. The company's in-house team of certified professionals ensures compliance with the latest codes, standards, and industry best practices—supported by responsive service and a dedication to long-term reliability.

Founded in 2009, Fire and Security Services Corporation continues to evolve with emerging solutions and technologies that keep clients secure, connected, and future-ready.

Our mission remains simple:
Providing Solutions for Your Fire & Security Needs™

FIRE AND SECURITY SERVICES